WHAT IS CLAIMED IS:

Sub a3

1. A public key infrastructure (PKI) comprising:

a subject;

a certificate authority issuing a first unsigned certificate to the subject that binds a public key of the subject to long-term identification information related to the subject, the certificate authority maintaining a certificate database of unsigned certificates in which it stores the first unsigned certificate; and

a verifier maintaining a hash table containing cryptographic hashes of valid unsigned certificates corresponding to the unsigned certificates stored in the certificate database and including a cryptographic hash of the first unsigned certificate, wherein the subject presents the issued first unsigned certificate to the verifier for authentication and demonstrates that the subject has knowledge of a private key corresponding to the public key in the unsigned certificate.

2. The PKI of claim 1 wherein the first unsigned certificate includes an expiration date/time.

3. The PKI of claim 1 wherein the first unsigned certificate does not include an expiration date/time.

4. The PKI of claim 1 wherein the private key is stored in a smartcard accessible by the subject.

5. The PKI of claim 1 wherein the private key is stored in a secure software wallet accessible by the subject.

6. The PKI of claim 1 wherein the verifier computes the cryptographic hash of the first unsigned certificate with a collision-resistant hash function.

7. The PKI of claim 6 wherein the collision-resistant hash function is a SHA-1 hash function.

8. The PKI of claim 6 wherein the collision-resistant hash function is a MD5 hash function.

9. The PKI of claim 1 wherein the certificate authority and the verifier operate to revoke the first unsigned certificate when the binding of the subject's public key to the long-term identification information related to the subject becomes invalid.

10. The PKI of claim 9 wherein the certificate authority and the verifier perform the revocation protocol to revoke the first unsigned certificate, the revocation protocol including:

the certificate authority retrieving first unsigned certificate from the certificate database and computing a cryptographic hash of the first unsigned certificate;

the certificate authority sending a message to verifier containing the cryptographic hash of the first unsigned certificate and requesting that the verifier remove the corresponding cryptographic hash of the first unsigned certificate from its hash table;

the verifier removing the cryptographic hash of the first unsigned certificate from its hash table and notifying the certificate authority that it has removed the cryptographic hash of the first unsigned certificate from its hash table; and

the certificate authority collecting the notification sent by the verifier.

11. The PKI of claim 10 wherein the revocation protocol includes the certificate authority marking the first unsigned certificate in the certificate database as being invalid, for auditing purposes.

12. The PKI of claim 10 wherein the revocation protocol includes the certificate authority deleting the first unsigned certificate from the certificate database.

13. A method of authenticating a subject to a verifier in a public key infrastructure (PKI), the method comprising the steps of:

issuing a first unsigned certificate from a certificate authority to the subject that binds a public key of the subject to long-term identification information related to the subject;

maintaining, at the certificate authority, a certificate database of unsigned certificates;

storing the first unsigned certificate in the certificate database;

maintaining, at the verifier, a hash table containing cryptographic hashes of valid unsigned certificates corresponding to the unsigned certificates stored in the certificate database and including a cryptographic hash of the first unsigned certificate;

presenting the issued first unsigned certificate from the subject to the verifier for authentication;

demonstrating, by the subject, that the subject has knowledge of a private key corresponding to the public key in the unsigned certificate.

14. The method of claim 13 wherein the first unsigned certificate includes an expiration date/time.

15. The method of claim 13 wherein the first unsigned certificate does not include an expiration date/time.

16. The method of claim 13 further comprising the step of:

storing the private key in a smartcard accessible by the subject.

17. The method of claim 13 further comprising the step of:

storing the private key in a secure software wallet accessible by the subject.

18. The method of claim 13 further comprising the step of:

computing, by the verifier, the cryptographic hash of the first unsigned certificate with a collision-resistant hash function.

19. The method of claim 18 wherein the collision-resistant hash function is a SHA-1 hash function.

20. The method of claim 18 wherein the collision-resistant hash function is a MD5 hash function.

21. The method of claim 13 further comprising the step of:

revoking the first unsigned certificate when the binding of the subject's public key to the long-term identification information related to the subject becomes invalid.

22. The method of claim 21 wherein the revoking step includes the steps of:

retrieving first unsigned certificate from the certificate database and computing a cryptographic hash of the first unsigned certificate;

sending a message from certificate authority to verifier containing the cryptographic hash of the first unsigned certificate;

requesting that the verifier remove the corresponding cryptographic hash of the first unsigned certificate from its hash table;

removing the cryptographic hash of the first unsigned certificate from the hash table;

notifying the certificate authority that the cryptographic hash of the first unsigned certificate is removed from the hash table; and

collecting, at the certificate authority, the notification sent in the notifying step.

23. The method of claim 22 wherein the revoking step further includes:

marking the first unsigned certificate in the certificate database as being invalid, for auditing purposes.

24. The method of claim 22 wherein the revoking step further includes:

deleting the first unsigned certificate from the certificate database.